Cyclotomic Polynomials
Klein Project session, MathFest 2010

Harriet Pollatsek
Mount Holyoke College
hpollats@mtholyoke.edu

August 9, 2010

Outline

This talk is really about factoring and finding roots of $x^n - 1$:

- Klein on Fermat's Last Theorem and Kummer (17th & 19th C)
- Klein on Gauss and constructing regular n-gons (18th & 19th C)
- $x^n - 1$ over a finite field, error-correcting codes (20th C)

What did Klein say?

Klein introduces these ideas via Fermat's Last Theorem.

If $x^n + y^n = z^n$ has an integer solution with $z \neq 0$, then

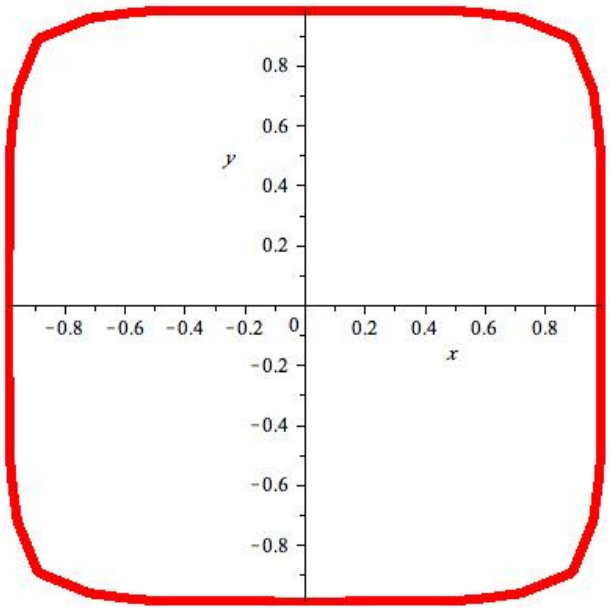
divide through by z^n and let $X = x/z$, $Y = y/z$ to see

$X^n + Y^n = 1$ has a rational solution.

Klein: think about FLT graphically

Think about the graph of $X^n + Y^n = 1$ in the plane.

For $n = 2$, the graph is a circle passing through infinitely many rational points. For $n > 2$?



For $n = 6$: the graph of $X^6 + Y^6 = 1$

Klein: Fermat's Last Theorem

Klein: Fermat's Last Theorem says that for $n \geq 3$

"these curves ... thread through the dense set of the rational

points without passing through a single one except "

the points where they intersect the coordinate axes.

Klein: Kummer and FLT

Klein next brings Kummer and $x^n - 1 = 0$ into the FLT story.

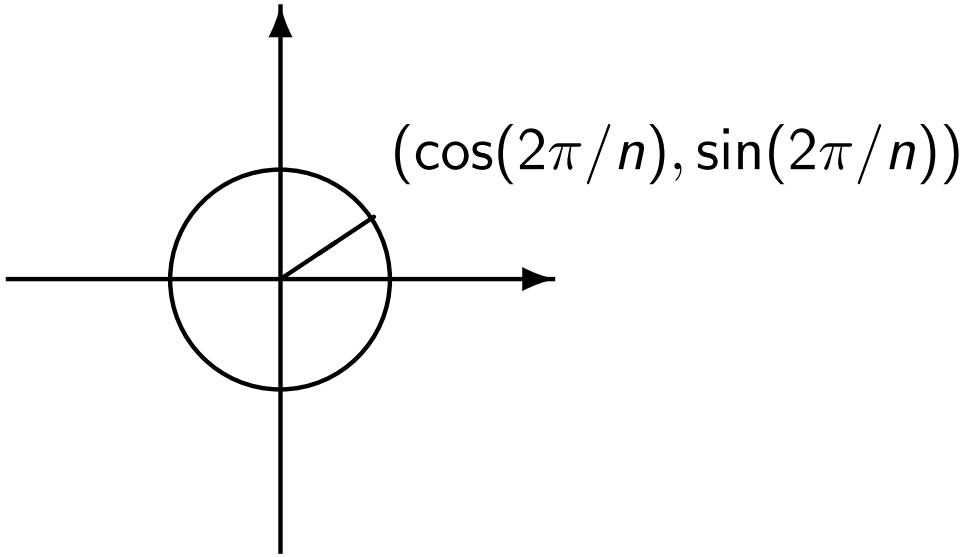
$x^n + y^n = z^n \Leftrightarrow$

$x^n = z^n - y^n = (z - y)(z - \varepsilon y)(z - \varepsilon^2 y) \cdots (z - \varepsilon^{n-1} y)$

for $\varepsilon = e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n)$

so $\varepsilon^n = 1$ by de Moivre's theorem

Klein: Kummer and cyclotomic numbers



Kummer called the complex roots of $x^n - 1$ cyclotomic numbers

(Greek: circle + cut) Also called nth roots of unity.

Cyclotomic polynomials: definition

$\varepsilon = e^{2\pi i/n} \Rightarrow \varepsilon^k$ for $k = 0, \ldots, n-1$ are the nth roots of unity,

and they mark the vertices of a regular n-gon on the unit circle.

$\omega \in \mathbb{C}$ is a primitive nth root of unity if

$\omega^n = 1$ and $\omega^m \neq 1$ for $0 < m < n$ ($\Leftrightarrow \omega = \varepsilon^k$ for $(k, n) = 1$).

Cyclotomic polynomials: definition

$\varepsilon = e^{2\pi i/n} \Rightarrow \varepsilon^k$ for $k = 0, \ldots, n-1$ are the nth roots of unity,

and they mark the vertices of a regular n-gon on the unit circle.

$\omega \in \mathbb{C}$ is a primitive nth root of unity if

$\omega^n = 1$ and $\omega^m \neq 1$ for $0 < m < n$ ($\Leftrightarrow \omega = \varepsilon^k$ for $(k, n) = 1$).

Define the nth cyclotomic polynomial $\Phi_n(x)$ by

$$\Phi_n(x) = \prod_{\omega} (x - \omega) \quad \omega \text{ varies over all primitive } n\text{th roots of } 1.$$

Cyclotomic polynomials: examples

$n = 4$: primitive roots are i and $-i$,

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1$$

$n = 5$: $\varepsilon = e^{2\pi i/5}$ and primitive roots are $\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$,

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$n = 6$: $\varepsilon = -e^{2\pi i/3}$, and primitive roots are ε and ε^5

$$\Phi_6(x) = x^2 - x + 1$$

Cyclotomic polynomials: basic facts

Proposition

1. *degree* $\Phi_n(x)$ *is* $\varphi(n) =$ *number of positive integers less than* n *and relatively prime to* n.
2. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
3. $\Phi_n(x)$ *has integer coefficients.*

Cyclotomic polynomials: surprising facts

Seductive but **FALSE**: the coefficients of $\Phi_n(x)$ are in $\{0, 1, -1\}$

True for $1 \leq n \leq 104$, false for $n = 105$

M. Isaacs in *Algebra: A Graduate Course*: "The author is unaware of any other 'simple' wrong conjecture that works for so many cases before failing."

Cyclotomic polynomials: surprising facts

Seductive but **FALSE**: the coefficients of $\Phi_n(x)$ are in $\{0, 1, -1\}$

True for $1 \leq n \leq 104$, false for $n = 105$

M. Isaacs in *Algebra: A Graduate Course*: "The author is unaware of any other 'simple' wrong conjecture that works for so many cases before failing."

Theorem

(J. Suzuki, 1987)
If $a(k, n)$ is the coefficient of x^k in $\Phi_n(x)$, then
$\{a(k, n) : k, n \in \mathbb{N}\} = \mathbb{Z}$.

Klein: Geometric constructions

Klein again: "I close my remarks about Fermat's theorem and come to . . . the problem of . . . construct[ing] a regular polygon of n sides."

Start with two points in the plane labeled **0** and **1**. What other points in the plane can be constructed with compass and straightedge?

Identify **0** with $(0, 0)$, **1** with $(1, 0)$, and points of plane with $\mathbb{C}$. Say $\alpha \in \mathbb{C}$ is constructible if $\alpha = a + bi$ and (a, b) is constructible.

Geometric constructions: Gauss

For n odd, the Greeks knew how to construct regular n-gons only for $n = 3$, 5 and $3 \times 5 = 15$.

Theorem

(Gauss, 1796) The regular 17-gon is constructible.

Proposition

A regular n-sided polygon is constructible if and only if $\varepsilon = e^{2\pi i/n}$ *is constructible.*

Geometric constructions: field theory

Theorem

α in $\mathbb{C}$ is constructible $\Leftrightarrow$ α is in the "splitting field" of an irreducible polynomial in $\mathbb{Q}[x]$ of degree 2^a for some a.

Theorem

(Gauss, 1798) For all n, $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Corollary

A regular n-gon is constructible $\Leftrightarrow$ $\varphi(n) = 2^a$ for some a.
$\Leftrightarrow$ $n = 2^b$ or $n = 2^b p_1 \cdots p_t$ for distinct Fermat primes p_j, $b \geq 0$.

A Fermat prime p has the form $2^m + 1$. Fermat knew exactly five, and so do we: 3, 5, 17, 257, 66537.

Factoring $x^n - 1$ over $GF(2)$: error-correcting codes

Mid 20th century:

Write $\mathbb{F} = GF(2) = \{0, 1\}$. $\mathbb{F}$ is students' dream field:

$+1 = -1$ and $(a + b)^2 = a^2 + b^2$ for $a, b \in \mathbb{F}$.

Error correcting codes (Richard Hamming, 1947):

$(x_1, x_2, x_3, x_4) \in \mathbb{F}^4 \longrightarrow (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{F}^7$, where
message codeword

x_5, x_6, x_7 depend linearly on x_1, x_2, x_3, x_4. (encoding)

The Code $\mathcal{C}$ is the solution space of the system of linear equations.

Error-correcting codes: minimum distance

For $\vec{v} \in \mathbb{F}^n$, the weight $wt(\vec{v})$ of $\vec{v}$ is number of nonzero coordinates of $\vec{v}$.

For $\vec{u}, \vec{w} \in \mathbb{F}^n$, the Hamming distance $d(\vec{u}, \vec{w}) = wt(\vec{u} - \vec{w})$.

t errors in $\vec{u}$ (changing t coordinates) gives $\vec{w} \Leftrightarrow d(\vec{u}, \vec{w}) = t$.

If the minimum nonzero weight of a vector in $\mathcal{C}$ is d

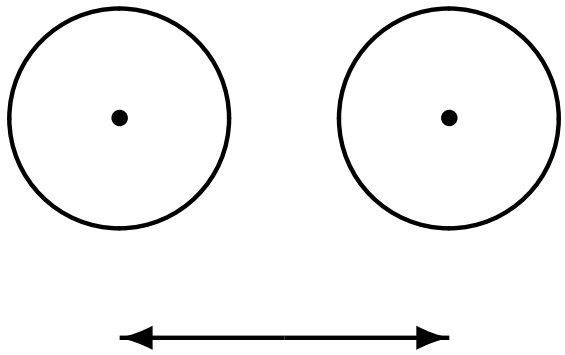
we say $\mathcal{C}$ has minimum distance d.

Hamming's code has dimension 4 and minimum distance 3.

Error-correcting codes: nearest neighbor decoding

Draw circles of radius $\lfloor (d-1)/2 \rfloor$ around each codeword.

Centers at distance $\geq d$ so circles disjoint!



distance d

"Nearest neighbor" decoding corrects up to $\lfloor (d-1)/2 \rfloor$ errors.

Hamming's code has $d = 3$ and corrects single errors.

Factoring $x^n - 1$ over $GF(2)$: cyclic codes

A code $\mathcal{C}$ is cyclic if
$(a_0, \ldots, a_{n-1}) \in \mathcal{C} \Leftrightarrow (a_{n-1}, a_0, \ldots, a_{n-2}) \in \mathcal{C}$

Sloane and MacWilliams: "Cyclic codes are the most studied of all codes." Encoding and decoding can be done very efficiently.

Associate $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}^n$ with

$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}[x]$.

Then $(a_{n-1}, a_0, \ldots, a_{n-2})$ corresponds to

$x(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1})$ modulo $x^n - 1$

(i.e., treat x^n as if it were 1)

Modular arithmetic/modular algebra

Arithmetic: Write $\langle 5 \rangle$ for the set of integer multiples of 5,

and $\mathbb{Z}/\langle 5 \rangle = \{0, 1, 2, 3, 4\}$ for the set of congruence classes of

integers mod 5. (i.e., treat 5 as if it were 0)

Algebra: Write $\langle x^n - 1 \rangle$ for the set of multiples of $x^n - 1$ in $\mathbb{F}[x]$,

and $R_n = \mathbb{F}[x]/\langle x^n - 1 \rangle$ for set of congruence classes

of polynomials mod $x^n - 1$ (i.e., treat $x^n - 1$ as if it were 0)

Factoring $x^n - 1$ over $GF(2)$: cyclic codes

Since $f(x), g(x)$ in $\mathcal{C} \Rightarrow f(x) + g(x)$ and $xg(x)$ in $\mathcal{C}$,

binary linear cyclic codes correspond to ideals in the ring R_n.

For code (ideal) $\mathcal{C}$ in R_n, choose $g(x)$ of least degree in $\mathcal{C}$.

Then $\mathcal{C} = \langle g(x) \rangle$ consists of all multiples of $g(x)$,

$g(x)$ is generator polynomial of $\mathcal{C}$.

Proposition

$g(x)$ is a factor of $x^n - 1$ in $\mathbb{F}[x]$ and $\dim \mathcal{C} = n - \deg g(x)$.

Factoring $x^n - 1$ over $GF(2^m)$: splitting field

Question: Minimum distance of $\mathcal{C}$?

It turns out that we need the linear factors of $x^n - 1$.

Proposition

When $n = 2^m - 1$, $GF(2^m)$ is the splitting field for $x^n - 1$ and

for every $g(x)$ in $\mathbb{F}[x]$ dividing $x^n - 1$.

Example: factoring $x^7 - 1$ over $GF(8)$

$n = 7$, $GF(8)^* = \langle \alpha \rangle$

$\alpha^7 = 1$ and $\alpha^3 + \alpha^2 + 1 = 0$.

$$x^7 - 1 = x^7 + 1 = (x+1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

$$= (x+1)(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6).$$

Factoring $x^n - 1$ over $GF(2)$: BCH codes

What about the minimum distance of the code generated by $g(x)$?
The most famous linear cyclic code is the BCH code

1959 Alexis Hocquenghem

1960 R.C. Bose and D.K. Ray-Chaudhuri

Theorem

(BCH bound)
Let $n = 2^m - 1$ and assume $GF(2^m)^* = \langle \alpha \rangle$. Choose $g(x)$ dividing $x^n - 1$ over $\mathbb{F}$ so that $g(x)$ is the product of the minimum polynomials of M consecutive powers of α. Let $\mathcal{C} = \langle g(x) \rangle$. Then the minimum distance of $\mathcal{C}$ is at least $M + 1$.

Factoring $x^7 - 1$: BCH codes with $n = 7$

β and β^2 in $GF(8)$ have the same minimum polynomial over $\mathbb{F}$.

Orbits of $\beta \mapsto \beta^2$ are zeroes of irred. factors of $x^7 - 1/\ \mathbb{F} \Rightarrow$

$\{1 = \alpha^0\} \quad \leftrightarrow \quad x + 1$ of degree 1

$\{\ \alpha,\ \alpha^2,\ \alpha^4\} \quad \leftrightarrow \quad a(x)$ of degree 3, $a(x) = x^3 + x^2 + 1$

$\{\alpha^3,\ \alpha^6,\ \alpha^{12} = \alpha^5\ \} \quad \leftrightarrow \quad b(x)$ of degree 3, $b(x) = x^3 + x + 1$

$\mathcal{C} = \langle\ a(x)\ \rangle$ with $M + 1 = 3 \Rightarrow \dim \mathcal{C} = 4$, $\mathcal{C}$ corrects 1 error.

$\mathcal{C} = \langle\ b(x)\ \rangle$ with $M + 1 = 3 \Rightarrow \dim \mathcal{C} = 4$, $\mathcal{C}$ corrects 1 error.

(both equivalent to Hamming's binary code of length 7)

Factoring $x^{15} - 1$: BCH code with $n = 15$

Orbits of $\beta \mapsto \beta^2$ in $GF(16) \Rightarrow$ irred. factors of $x^{15} - 1/\ \mathbb{F}$:

$\{1 = \alpha^0\}$ $\leftrightarrow$ $x + 1$ of degree 1

$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ $\leftrightarrow$ $a(x)$ of degree 4

$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9\}$ $\leftrightarrow$ $b(x)$ of degree 4

$\{\alpha^5, \alpha^{10}\}$ $\leftrightarrow$ $c(x)$ of degree 2

$\{\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{56} = \alpha^{11}\}$ $\leftrightarrow$ $d(x)$ of degree 4

$g(x) = a(x)b(x)c(x)$ with $M + 1 = 7 \Rightarrow$

$\dim \mathcal{C} = 15 - 10 = 5$, $d = 7$ and $\mathcal{C}$ corrects 3 errors.

BCH code [15, 5, 7]: generator polynomial

What is $g(x)$ and is it really in $\mathbb{F}[x]$?

From addition table for $GF(16)$ in *Introduction to the Theory of Error-Correcting Codes* by V. Pless:

$$a(x) = x^4 + x^3 + 1$$

$$b(x) = x^4 + x^3 + x^2 + x + 1$$

$$c(x) = x^2 + x + 1$$

$$g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$$

How good are BCH codes?

Suppose we have an infinite family $\mathcal{C}_j$, $j = 1, 2, \ldots$, of linear codes defined over $\mathbb{F}$.

Assume the code $\mathcal{C}_j$ is a k_j-dimensional subspace of $\mathbb{F}^{n_j}$ and has minimum distance d_j.

The family is good if both k_j/n_j and d_j/n_j have positive limits as $j \to \infty$.

Unfortunately, the family of BCH codes is not good. (See F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, page 269.)